MODELING AND ANALYSIS OF INFORMATION SYSTEMS, VOL. 27, NO. 1, 2020

journal homepage: www.mais-journal.ru

THEORY OF DATA

On the Properties of Algebraic Geometric Codes as Copy Protection Codes

V. M. Deundyak[1;2], D. V. Zagumennov[1]

DOI: 10.18255/1818-1015-2020-1-22-38

[1]Southern Federal University, 105/42 Bolshaya Sadovaya str., Rostov-on-Don 344006, Russia.
[2]FGNU NII Specvusavtomatika, 51 Gazetniy lane, Rostov-on-Don 344002, Russia.

MSC2020: 94B27
Research article
Full text in Russian

Received November 19, 2019
After revision February 17, 2020
Accepted February 28, 2020

Traceability schemes which are applied to the broadcast encryption can prevent unauthorized parties from accessing the distributed data. In a traceability scheme a distributor broadcasts the encrypted data and gives each authorized user unique key and identifying word from selected error-correcting code for decrypting. The following attack is possible in these schemes: groups of c malicious users are joining into coalitions and gaining illegal access to the data by combining their keys and identifying codewords to obtain pirate key and codeword. To prevent this attacks, classes of error-correcting codes with special c-FP and c-TA properties are used. In particular, c -FP codes are codes that make direct compromise of scrupulous users impossible and c -TA codes are codes that make it possible to identify one of the attackers. We are considering the problem of evaluating the lower and the upper boundaries on c, within which the L-construction algebraic geometric codes have the corresponding properties. In the case of codes on an arbitrary curve the lower bound for the c-TA property was obtained earlier; in this paper, the lower bound for the c-FP property was constructed. In the case of curves with one infinite point, the upper bounds for the value of c are obtained for both c-FP and c-TA properties. During our work, we have proved an auxiliary lemma and the proof contains an explicit way to build a coalition and a pirate identifying vector. Methods and principles presented in the lemma can be important for analyzing broadcast encryption schemes robustness. Also, the c-FP and c-TA boundaries monotonicity by subcodes are proved.

Keywords: error-correcting codes; traceability schemes; algebraic geometry codes

INFORMATION ABOUT THE AUTHORS

Vladimir M. Deundyak correspondence author	orcid.org/0000-0001-8258-2419. E-mail: vl.deundyak@gmail.com PhD.
Denis V. Zagumennov	orcid.org/0000-0001-8990-9058. E-mail: zagumionnov.denis@yandex.ru graduate student.

For citation: V. M. Deundyak and D. V. Zagumennov, “On the Properties of Algebraic Geometric Codes as Copy Protection Codes”, *Modeling and analysis of information systems*, vol. 27, no. 1, pp. 22-38, 2020.

МОДЕЛИРОВАНИЕ И АНАЛИЗ ИНФОРМАЦИОННЫХ СИСТЕМ, ТОМ 27, № 1, 2020
сайт журнала: www.mais-journal.ru

THEORY OF DATA

Исследование свойств АГ-кодов как кодов для защиты от копирования

В. М. Деундяк[1;2], Д. В. Загуменнов[1]

DOI: 10.18255/1818-1015-2020-1-22-38

[1]Южный Федеральный Университет, ул. Большая Садовая, 105/42, Ростов-на-Дону, 344006, Россия.
[2]ФГНУ НИИ Спецвузавтоматика, пер. Газетный, 51, Ростов-на-Дону, 344002, Россия.

УДК 519.7
Научная статья
Полный текст на русском языке

Получена 19 ноября 2019 г.
После доработки 17 февраля 2020 г.
Принята к публикации 28 февраля 2020 г.

Схемы специального широковещательного шифрования используются для защиты легально тиражируемой цифровой продукции от несанкционированного копирования. В таких схемах распространитель тиражирует данные свободно в зашифрованном виде, а для расшифрования выдаёт каждому легальному пользователю уникальный набор ключей и идентифицирующих векторов из некоторого помехоустойчивого кода. Однако, в этих схемах возможна атака, в ходе которой группы из c недобросовестных пользователей могут объединяться в коалиции и получать нелегальный доступ к данным, комбинируя выданную им ключевую информацию для получения пиратской ключевой информации — идентификационного вектора и ключа. Для борьбы с коалиционными атаками применяются классы помехоустойчивых кодов, обладающих специальными c-FP и c-TA свойствами. Класс c-FP-кодов составляют коды, исключающие возможность прямой компрометации добросовестных пользователей, а класс c-TA-кодов составляют коды, позволяющие гарантированно определить одного из злоумышленников. Рассматривается задача нахождения нижних и верхних границ значения величины c, в пределах которых алгеброгеометрические коды L-конструкции обладают соответствующими свойствами. В случае кодов на произвольной кривой ранее была получена нижняя граница для свойства c-TA, в настоящей работе построена нижняя граница для свойства c-FP. В случае кривых с одной бесконечной точкой получены верхние границы значения c как для c-FP, так и для c-TA свойств. При нахождении этих границ получена вспомогательная конструктивная лемма, в доказательстве которой содержится явный способ построения коалиции и пиратского идентификационного вектора; этот способ важен при анализе стойкости схем широковещательного шифрования. Доказаны свойства монотонности рубежей c-FP и c-TA свойств по подкодам.

Ключевые слова: помехоустойчивое кодирование; широковещательное шифрование; алгеброгеометрические коды

ИНФОРМАЦИЯ ОБ АВТОРАХ

Владимир Михайлович Деундяк
автор для корреспонденции
orcid.org/0000-0001-8258-2419. E-mail: vl.deundyak@gmail.com
канд. физ.-мат. наук, доцент.

Денис Владимирович Загуменнов
orcid.org/0000-0001-8990-9058. E-mail: zagumionnov.denis@yandex.ru
аспирант.

Для цитирования: V. M. Deundyak and D. V. Zagumennov, “On the Properties of Algebraic Geometric Codes as Copy Protection Codes”, *Modeling and analysis of information systems*, vol. 27, no. 1, pp. 22-38, 2020.

Введение

В работе рассматривается перспективный способ применения помехоустойчивых АГ-кодов L-конструкции в качестве кодов для защиты легально тиражируемой цифровой продукции от несанкционированного копирования [1], который называется схемой специального широковещательного шифрования (ССШШ). В этих схемах распространитель тиражирует данные свободно в зашифрованном виде, а каждому легальному пользователю для расшифрования данных выдаёт уникальный набор ключей и идентифицирующих векторов из соответствующего помехоустойчивого кода. В ССШШ пользователи применяют кодовые идентифицирующие векторы при выполнении легального доступа к данным. В случае обнаружения нелегального использования ключевой информации её владелец может быть идентифицирован контролёром. В ССШШ возможны атаки следующего вида: некоторые недобросовестные легальные пользователи могут объединяться в коалиции злоумышленников некоторой мощности $c \in \mathbb{N} \setminus \{1\}$ с целью создания пиратских идентифицирующих векторов и ключей, которые можно использовать для выполнения нелегального доступа к данным, что может привести к различным злоупотреблениям. Для борьбы с подобными атаками в [1—3] предложен метод обнаружения членов коалиций, основанный на использовании некоторых классов линейных кодов, описание и анализ эффективности подобных схем приведён также в [4].

Для использования в таких системах в настоящее время активно исследуются и применяются классы так называемых c-TA и c-FP-кодов для защиты от несанкционированного копирования. Класс c-TA-кодов составляют такие коды, для которых применение к пиратскому идентификационному вектору любого декодера, работающего по минимуму кодового расстояния, позволяет гарантированно найти идентификационный вектор злоумышленника, входящего в атакующую коалицию мощности c. Более широкий класс c-FP-кодов составляют такие коды, для которых пиратский идентификационный вектор, созданный коалицией мощности c, не может являться идентификационным вектором пользователя, не входящего в коалицию, что исключает возможность прямой компрометации невиновных пользователей.

Актуальными представляются задачи поиска новых классов помехоустойчивых кодов для дальнейшего их использования в ССШШ, а также уточнения рубежей, при которых выполнены свойства c-TA и c-FP. В [3] показана возможность применения некоторых кодов Рида-Соломона в качестве c-TA-кодов, а в [5] исследованы рубежи значения c для кодов Рида-Соломона, при которых они являются c-TA и c-FP-кодами. В работе [6] показана возможность применения q-ичных кодов Рида-Малера в качестве как c-TA, так и c-FP-кодов, а также исследованы соответствующие рубежи. В [3] показана возможность применения некоторых алгеброгеометрических кодов (АГ-кодов) L-конструкции, а в [7] получены достаточные условия наличия свойства c-TA у АГ-кодов, а также условия применимости в ССШШ некоторых списочных декодеров для АГ-кодов L-конструкции.

В настоящей статье вычислена нижняя граница для рубежа c-FP свойства в случае АГ-кодов на произвольных кривых и доказана монотонность рубежей c-FP свойства и c-TA свойства по подкодам. Для АГ-кодов на специальных классах кривых с одной бесконечной точкой вычислены верхние границы рубежей как для c-FP, так и для c-TA свойства.

1. Классы c-TA и c-FP-кодов

Ниже будем использовать стандартные обозначения из теории кодирования (см. [8]). Пусть C – линейный $[n, k, d]_q$ код, $x, y \in C$,

$$I(x, y) = \{i \in \mathbb{N} \,:\, 1 \le i \le n, x_i = y_i\};$$

ясно, что $|I(x, y)| = n - d(x, y)$, где $d(x, y)$ – расстояние Хэмминга между x и y.

Пусть $c \in \mathbb{N} \setminus \{1\}$. Коалицией кода C назовём множество $C_0 = \{u_1, u_2, \dots, u_c\}$, где $u_i \in C$. Число cбудем называть мощностью коалиции, а множество коалиций кода C мощности не больше c будем

обозначать как $\mathrm{coal}_c(C)$. Ясно, что c существенно меньше мощности кода C. Множеством потомков коалиции C_0 назовём множество

$$\mathrm{desc}(\mathrm{C}_0) = \{(y_1, y_2, , \dots, y_n) \in \mathbb{F}_q^n \mid y_j = u_{i,j},\ i \in \{1, \dots, c\},\ j \in \{1, \dots, n\}\}.$$

Линейный код C называется c-ТА кодом ([1], определение 1.1), если выполняется следующее условие:

$$\forall\ C_0 \in \mathrm{coal}_c(C)\ \ \forall\ v \in (C \setminus C_0)\ \ \forall\ y \in \mathrm{desc}(\mathrm{C}_0)\ \ \exists\ \omega \in C_0\ d(w, y) < d(v, y).$$

Отметим, что если для кода C выполнено c-ТА-свойство, то для любого вектора $v \in C$ ни одна коалиция мощности не более c не сможет комбинированием элементов своих кодовых векторов сгенерировать потомка ω, находящегося ближе к v, чем к этой коалиции. Множеством ТА-компрометации для кода C называется множество:

$$\Omega_{TA}(C) = \{c \in \mathbb{N}_1 \ :\ \exists v \in C\ \exists C_0 \in \mathrm{coal}_c(C \setminus \{v\})\ \exists \omega \in \mathrm{desc}(C_0) \setminus C_0\ \forall u \in C_0\ :\ d(v, \omega) \le d(u, \omega)\}$$

(см. [6], с. 101). Таким образом, для того, чтобы доказать, что для кода C не выполнено c-ТА-свойство, достаточно построить кодовый вектор v, коалицию C_0 мощности максимум c и потомка этой коалиции ω такие, чтобы расстояние от этого потомка ω до v было меньше, чем расстояние от этого потомка ω до любого из членов коалиции.

Линейный код C будем называть c-FP кодом ([1], определение 1.1), если выполняется следующее условие:

$$\forall\ C_0 \in \mathrm{coal}_c(C)\ \ \forall\ z \in (C \setminus C_0)\ :\ z \notin \mathrm{desc}(C_0) \setminus C_0.$$

Таким образом, если для кода C выполнено c-FP-свойство, то ни одна коалиция мощности не более c не сможет комбинированием элементов своих кодовых векторов сгенерировать другой кодовый вектор. Множеством FP-компрометации для кода C называется множество:

$$\Omega_{FP}(C) = \{c \in \mathbb{N}_1 \ :\ \exists C_0 \in \mathrm{coal}_c(C)\ \exists z \in (C \setminus C_0)\ :\ z \in \mathrm{desc}(C_0) \setminus C_0\ (z \in \mathrm{desc}(C_0))\}$$

(см. [6], с. 101). Таким образом, для того, чтобы доказать, что для кода C не выполнено c-FP-свойство, достаточно построить коалицию мощности не более c и кодовый вектор такие, чтобы этот кодовый вектор являлся потомком этой коалиции.

Множества $\Omega_{TA}(C)$ и $\Omega_{FP}(C)$ являются целочисленными отрезками:

$$\Omega_{TA}(C) = \{R_{TA}(C), R_{TA}(C) + 1, \dots\},$$

$$\Omega_{FP}(C) = \{R_{FP}(C), R_{FP}(C) + 1, \dots\}.$$

Величины $R_{TA}(C)$ и $R_{FP}(C)$ будем называть рубежами множеств компрометации. Из определений вытекают следующие вложение и неравенство:

$$\Omega_{FP}(C) \subseteq \Omega_{TA}(C),\ R_{TA}(C) \le R_{FP}(C) \tag{1}$$

Докажем лемму о монотонности свойств ТА и FP.

Лемма 1. *Пусть C_1 и C_2 – линейные коды в $\mathbb{F}_q^n$, и C_1 – подкод C_2. Тогда выполняется:*

$$R_{TA}(C_1) \ge R_{TA}(C_2),\ \ R_{FP}(C_1) \ge R_{FP}(C_2).$$

Доказательство. Пусть $c \in \mathbb{N} \setminus \{1\}$, такое, что:

$$\exists v_1 \in C_1 \, \exists C^1 \in \mathrm{coal}_c(C_1 \setminus \{v_1\}) \, \exists \omega_1 \in \mathrm{desc}(C^1) \setminus C^1 \, \forall u \in C^1 \, : \, d(v_1, \omega_1) \leq d(u, \omega_1).$$

Тогда, учитывая, что $C_1 \subset C_2$, получаем, что

$$\exists v_2 \in C_2 = v_1 \, \exists C^2 \in \mathrm{coal}_c(C_2 \setminus \{v_2\}) = C^1 \, \exists \omega_2 \in \mathrm{desc}(C^2) \setminus C^2 = \omega_1 \, \forall u \in C^2 \, : \, d(v_2, \omega_2) \leq d(u, \omega_2).$$

Таким образом, если для $c \in \mathbb{N} \setminus \{1\}$ не выполняется c-ТА свойства для кода C_1, то c-ТА свойство не выполняется и для кода C_2, значит, $R_{TA}(C_1) \geq R_{TA}(C_2)$.

Аналогично доказывается и второе неравенство. □

Для кодов Рида-Маллера аналогичная лемма доказана в [9] (теоремы 2 и 4).

2. Алгеброгеометрические коды L-конструкции

2.1. Основные понятия

Ниже будем использовать подходы к АГ-кодам L-конструкции из [10, 11]. Рассмотрим конечное поле $\mathbb{F}_q$ и кольца многочленов $\mathbb{F}_q[x_1, x_2]$, $\mathbb{F}_q[X_1, X_2, X_3]$. Обозначим через $\mathbb{F}_q^{\mathrm{hom}}[X_1, X_2, X_3]$ множество однородных многочленов из $\mathbb{F}_q[X_1, X_2, X_3]$.

Отметим, что между многочленами f из $\mathbb{F}_q[x_1, x_2]$ и однородными многочленами F из $\mathbb{F}_q^{\mathrm{hom}}[X_1, X_2, X_3]$ существует взаимно-однозначное соответствие ([11], стр. 106-107), определяемое по следующему правилу. Если d – максимальная степень одночлена в многочлене $f \in \mathbb{F}_q[x_1, x_2]$, то F получается из f заменой каждого одночлена вида $x_1^i x_2^j$ на одночлен вида $X_1^i X_2^j X_3^{d-i-j}$. Это соответствие называется проективизацией.

Если точка P имеет аффинные координаты (a_1, a_2), то проективные координаты этой точки будем записывать так $(a_1 : a_2 : 1)$, в случае бесконечной точки третья проективная координата равна нулю ([10], с.7-8). Пусть $F \in \mathbb{F}_q^{\mathrm{hom}}[X_1, X_2, X_3]$, $\mathcal{X} = \mathcal{X}(F, \mathbb{F}_q)$ – плоская гладкая проективная кривая над полем $\mathbb{F}_q$, заданная неприводимым многочленом $F \in \mathbb{F}_q^{\mathrm{hom}}[X_1, X_2, X_3]$([11], п. 2.1.2). Далее в тексте будем рассматривать только такие кривые. Кривые имеют параметр $g \in \mathbb{N} \cup \{0\}$, называемый родом. В случае плоских гладких кривых род вычисляется по известной формуле ([11], следствие 2.2.8):

$$g = \frac{(\deg(F) - 1)(\deg(F) - 2)}{2}.$$

Через (F) обозначим главный идеал в $\mathbb{F}_q[X_1, X_2, X_3]$, порождённый F. В кольце

$$R = \left\{ \frac{P}{Q} \, : \, P, Q \in \mathbb{F}_q^{\mathrm{hom}}[X_1, X_2, X_3], \deg(P) = \deg(Q), Q \notin (F) \right\}$$

с естественными операциями сложения и умножения рассмотрим максимальный идеал

$$I = \left\{ \frac{P}{Q} \, : \, P, Q \in \mathbb{F}_q^{\mathrm{hom}}[X_1, X_2, X_3], \deg(P) = \deg(Q), Q \notin (F), P \in (F) \right\}$$

([11], п. 2.5.4). Тогда фактор-кольцо R/I является полем, оно называется полем рациональных функций на кривой $\mathcal{X}$ и обозначается $\mathbb{F}_q(\mathcal{X})$.

Согласно [11] (п. 2.5.2):

$$\forall M \in \mathcal{X} \, \exists T \in \mathbb{F}_q(\mathcal{X}) \, \forall H \in \mathbb{F}_q(\mathcal{X}) \exists U \in \mathbb{F}_q(\mathcal{X}) \, : \, T(M) = 0, U(M) \neq 0 \, : \, H = T^m U,$$

где $m \in \mathbb{Z}$, и значение величины m не зависит от выбора элемента T. Порядком $H = T^m U \in \mathbb{F}_q(\mathcal{X})$ в точке $M \in \mathcal{X}$ назовём значение величины m и будем обозначать это так: $\mathrm{ord}_M(H) = m$.

Дивизором D на проективной кривой $\mathcal{X}$ называется формальная сумма следующего вида: $D = \sum_{M\in\mathcal{X}} a_M M, a_M \in \mathbb{Z}$. Носителем дивизора называют множество $\mathrm{supp}(D) = \{M \in \mathcal{X} : a_M \neq 0\}$, а степенью дивизора D – число $\deg(D) = \sum a_M$. Если $\deg(D) = \alpha$, то иногда будем вместо D писать D_α. Говорят, что дивизор

$$D = \sum a_M M, a_M \in \mathbb{Z}, M \in \mathcal{X}$$

эффективен, если все $a_M \geq 0$. Этот факт обозначается следующим образом: $D \geq 0$. Дивизором функции $H \in \mathbb{F}_q(X)$ на проективной кривой $\mathcal{X}$ называется дивизор:

$$(H) = \sum_{M\in\mathcal{X}} \mathrm{ord}_M(H)M.$$

Для каждого $M \in \mathcal{X}$ рассмотрим произвольный линейный однородный многочлен $L \in \mathbb{F}_q^{\mathrm{hom}}[X_1, X_2, X_3]$, для которого $L(M) \neq 0$, и многочлен $G \in \mathbb{F}_q^{\mathrm{hom}}[X_1, X_2, X_3]$, у которого $\deg(G) = r$. Пусть $I(M; \mathcal{X}; G) = \mathrm{ord}_M(G/L^r)$ (см. [10], определение 2.22). Дивизором пересечения G и $\mathcal{X}$ называется дивизор вида

$$\mathcal{X} \cdot G = \sum_{M\in\mathcal{X}} I(M; \mathcal{X}; G)M. \tag{2}$$

Зафиксируем дивизор $D = \sum_{M\in\mathcal{X}} a_M M$. Множество

$$L(D) = \{H \in \mathbb{F}_q(\mathcal{X}) : (H) + D \geq 0\}$$

называется пространством Римана-Роха, ассоциированным с D. Пространство $L(D)$ является конечномерным векторным пространством ([10], теорема 2.37).

Пусть $P = \{P_1, \ldots, P_n\} \subset \mathcal{X}, D = \sum_{M\in\mathcal{X}} a_M M, \deg(D) = \alpha$ и $\mathrm{supp}(D) \cap P = \emptyset$. Образ отображения

$$Ev_P : L(D) \longrightarrow \mathbb{F}_q^n, Ev_P(H) = (H(P_1), H(P_2), \ldots, H(P_n)) \tag{3}$$

называется АГ-кодом L-конструкции. Обозначим его через $C(\mathcal{X}, P, D_\alpha)$. Дивизор D_α будем называть дивизором кода C.

Теорема 1 ([11], теорема 4.1.1). *Пусть $\mathcal{X}$ – плоская гладкая проективная кривая рода g, $0 < \alpha < n$. Тогда АГ-код $C(\mathcal{X}, P, D_\alpha)$ является $[n, k, d]_q$-кодом, где $k \geq \alpha - g + 1$, $d \geq n - \alpha$. Если $\alpha > 2g - 2$, то $k = \alpha - g + 1$.*

Замечание 1. *В случае, когда род кривой $\mathcal{X}$ над полем $\mathbb{F}_q$ равен нулю, а $\deg(F) = 1$, т.е. $\mathcal{X}$ – проективная прямая, то АГ-код $C = C(\mathcal{X}, P, D_\alpha)$ является $[q, \alpha + 1, q - \alpha]_q$-кодом Рида-Соломона ([11], пример 4.1.5).*

2.2. Монотонность свойств c-TA и c-FP

Введём на множестве дивизоров на кривой $\mathcal{X}$ отношение $\geq$ следующим образом. Пусть D^1 и D^2 – дивизоры на кривой $\mathcal{X}$, $D^1 = \sum_{M\in\mathcal{X}} a_M M$, $D^2 = \sum_{M\in\mathcal{X}} b_M M$. Тогда положим, что $D^2 \geq D^1$, если

$$D^2 - D^1 \geq 0.$$

Теорема 2. *Пусть D^1 и D^2 – дивизоры на кривой $\mathcal{X}(F, \mathbb{F}_q)$ и $D^2 \geq D^1$. Пусть $C_i = C(\mathcal{X}, P, D^i_\alpha)$, $i = 1, 2$. Тогда 1) код $C_1 = C(\mathcal{X}, P, D^1_\alpha)$ является подкодом $C_2 = C(\mathcal{X}, P, D^2_\alpha)$, 2) $R_{TA}(C_1) \geq R_{TA}(C_2)$, 3) $R_{FP}(C_1) \geq R_{FP}(C_2)$.*

Доказательство. 1) Рассмотрим произвольный элемент $f \in \mathbb{F}_q(\mathcal{X})$. Учитывая, что $D^2 \geq D^1$, легко проверить, что если $(f) + D^1 \geq 0$, то и $(f) + D^2 \geq 0$. Тогда из определения пространства Римана-Роха вытекает, если $f \in L(D^1)$, то $f \in L(D^2)$, значит, $L(D^1) \subset L(D^2)$. Таким образом, выполняется нужное вложение.

Доказательства утверждений 2) и 3) вытекает из утверждения 1) и леммы 1. □

3. Границы для свойства c-FP

Сформулируем теорему о границах множества компрометации для c-FP-свойства.

Теорема 3. *Пусть $\mathcal{X} = \mathcal{X}(F, \mathbb{F}_q)$ – плоская гладкая проективная кривая. Рассмотрим АГ-код $C = C(\mathcal{X}, P, D_\alpha)$. Тогда*

$$R_{FP}(C) \geq \left\lceil \frac{n}{\alpha} \right\rceil.$$

Если Q – единственная бесконечная точка на $\mathcal{X}$, $|P| > 1$, а $D = \alpha Q$, то:

$$R_{FP}(C) \leq B_{FP}(C) = \left\lceil \frac{n}{\lfloor \frac{\alpha}{\deg(F)} \rfloor} \right\rceil.$$

Если род кривой $\mathcal{X}$ равен нулю, а $\deg(F) = 1$, т.е. код является кодом Рида-Соломона (см. замечание 1), то оценки в теореме превращаются в равенство $R_{FP} = \lceil n/\alpha \rceil$ из [5].

Доказательство этой теоремы проведём после нескольких вспомогательных лемм.

Лемма 2. *Рассмотрим АГ-код $C = C(\mathcal{X}(F, \mathbb{F}_q), P, D_\alpha)$. Тогда:*

$$\forall c \in \mathbb{N} \setminus \{1\}\ \forall v \in C\ \forall C_0 \in \mathrm{coal}_c(C \setminus \{v\})\ \forall \omega \in \mathrm{desc}(C_0) \setminus C_0 \ :\ |I(\omega, v)| \leq \min\{\alpha c, n\}.$$

Доказательство. Пусть $c \in \mathbb{N} \setminus \{1\}$, $v \in C$ – произвольное кодовое слово, $C_0 = \{u_1; \dots; u_c\} \in \mathrm{coal}_c(C \setminus v)$ – произвольная коалиция, $\omega \in \mathrm{desc}(C_0) \setminus C_0$ – произвольный потомок коалиции C_0. Очевидно, что $|I(\omega, v)| \leq n$. Для доказательства леммы достаточно показать, что если $\min\{\alpha c, n\} = \alpha c$, то выполняется оценка $|I(\omega, v)| \leq \alpha c$.

Теперь предположим, что $\min\{\alpha c, n\} = \alpha c$, но $|I(\omega, v)| > \alpha c$. Так как ω – потомок коалиции C_0, то для каждого номера $j \in I(\omega, v)$ найдётся такой номер $i \in \{1, \dots, c\}$, что $v_j = \omega_j = u_{ij}$. Так как мощность коалиции C_0 равна c, то существует номер $\hat{i} \in \{1, \dots, c\}$, такой, что $|I(u_{\hat{i}}, v)| > \alpha$. Тогда ввиду того, что $u_{\hat{i}}, v \in C$ получим, что:

$$d(u_{\hat{i}}, v) = n - |I(u_{\hat{i}}, v)| < n - \alpha = d^*,$$

чего не может быть согласно теореме 1. Значит, $|I(\omega, v)| \leq \alpha c$. Таким образом, $|I(\omega, v)| \leq \min\{\alpha c, n\}$. □

Для дальнейшего нам понадобятся некоторые вспомогательные конструкции. Пусть $\mathcal{X} = \mathcal{X}(F, \mathbb{F}_q)$ – плоская гладкая проективная кривая, $P = \{P_1, \dots, P_n\}$ – множество всех точек вида $P_i = (P_{i,1} : P_{i,2} : 1)$ на кривой. Назовём это множество множеством конечных точек кривой. Введём на нём два отношения эквивалентности:

$$P_i \sim_1 P_j \iff P_{i,1} = P_{j,1},\ P_i \sim_2 P_j \iff P_{i,2} = P_{j,2}.$$

Отношение $\sim_1$ разбивает P на классы эквивалентности:

$$P/\sim_1 = \{R^1, \dots, R^{k_1}\},$$

$$R^i = \{R^i_1 = (R^i_{1,1} : R^i_{1,2} : 1), R^i_2 = (R^i_{2,1} : R^i_{2,2} : 1), \dots, R^i_{l_i} = (R^i_{l_i,1} : R^i_{l_i,2} : 1)\}, \tag{4}$$

отношение $\sim_2$ разбивает P на классы эквивалентности:

$$P/\sim_2 = \{S^1, \dots, S^{k_2}\},$$

$$S^i = \{S^i_1 = (S^i_{1,1} : S^i_{1,2} : 1), S^i_2 = (S^i_{2,1} : S^i_{2,2} : 1), \dots S^i_{m_i} = (S^i_{m_i,1} : S^i_{m_i,2} : 1)\}, \tag{5}$$

где R^i_j, S^i_j – точки из P, l_i, m_i – мощности факторклассов R^i и S^i соответственно.

Значение k_1 назовём индексом множества P по первой координате, а значение k_2 индексом множества P по второй координате. Очевидно, что $k_1 \le n, k_2 \le n$. Легко проверить, если оба индекса равны 1, то множество P состоит из одной точки. Таким образом, если $|P| > 1$, то один из индексов k_1, k_2 также больше 1.

Сформулируем и докажем следующую ключевую техническую лемму, доказательство которой является громоздким.

Лемма 3. *Пусть $\mathcal{X} = \mathcal{X}(F, \mathbb{F}_q)$ – плоская гладкая проективная кривая. Рассмотрим АГ-код $C = C(\mathcal{X}(F, \mathbb{F}_q), P, D_\alpha)$, где Q – единственная бесконечная точка на $\mathcal{X}$, $|P| > 1$, $D = \alpha Q$. Тогда:*

$$\forall c \in \mathbb{N} \setminus \{1\}\ \forall v \in C\ \exists C_0 \in \mathrm{coal}_c(C \setminus \{v\})\ \exists \omega \in \mathrm{desc}(C_0) \setminus C_0\ :\ |I(\omega, v)| \ge \min\{c \left\lfloor \tfrac{\alpha}{\deg(F)} \right\rfloor, n\} \quad (6)$$

Доказательство. Предположим, что лемма доказана для $v = 0$, т.е. мы можем построить коалицию $\hat{C}_0 = \{\hat{u}_1, \dots, \hat{u}_c\}$, такую, что:

$$\forall c \in \mathbb{N} \setminus \{1\}\ \exists\ \omega \in \mathrm{desc}(\hat{C}_0) \setminus \hat{C}_0\ :\ |I(\omega, 0)| \ge \min\{c \left\lfloor \frac{\alpha}{\deg(F)} \right\rfloor, n\}.$$

Рассмотрим произвольный вектор $v \in C$, коалицию $C_0 = \{\hat{u}_1 + v, \dots, \hat{u}_c + v\}$ и вектор $\omega = \hat{\omega} + v$. Так как C – линейный код, то $C_0 \in \mathrm{coal}_c(C \setminus \{v\})$, $\omega \in \mathrm{desc}(C_0) \setminus C_0$, и выполняется:

$$|I(\omega, v)| \ge \min\{c \left\lfloor \frac{\alpha}{\deg(F)} \right\rfloor, n\}.$$

Таким образом, если лемма справедлива для $v = 0$, то она справедлива и для любых других $v \in C$.

Докажем теперь лемму в предположении, что $v = 0$. Пусть $\delta = \left\lfloor \frac{\alpha}{\deg(F)} \right\rfloor$.

Рассмотрим сначала случай, когда $c\delta < n$, и разобьём доказательство на несколько шагов.

I. Рассмотрим множество $P \subset \mathcal{X}$. Так как по построению АГ-кода $\mathrm{supp}(D) \cap P = \emptyset$, $\mathrm{supp}(D) = \{Q\}$, и Q – единственная бесконечная точка на кривой $\mathcal{X}$, то в P нет бесконечных точек, т.е. точек вида $(X_1 : X_2 : 0)$. Значит, множество P является подмножеством множества конечных точек кривой, причём, т.к. $|P| > 1$, то один из индексов P больше единицы (см. (4), (5)). Не нарушая общности, будем считать, что k_1 больше 1, и рассмотрим классы эквивалентности R^i. Перенумеруем множество P так, чтобы для первых k_1 точек из P выполняется условие: $P_i \in R^i,\ i \in \{1, \dots, k_1\}$.

II. Так как коалиция является набором кодовых векторов, каждый из которых является образом некоторой рациональной функции из пространства Римана-Роха $L(D)$ при кодирующем отображении, то для построения искомой коалиции необходимо сначала предъявить соответствующий набор рациональных функций.

Для искомых рациональных функций построим сначала вспомогательные многочлены. Рассмотрим несколько случаев.

a) Пусть $c\delta \le k_1$. Тогда в кольце $\mathbb{F}_q[x_1, x_2]$ рассмотрим следующие многочлены (см. (4)):

$$r_i(x_1, x_2) = (x_1 - R^{(i-1)\delta+1}_{1,1}) \dots (x_1 - R^{i\delta}_{1,1}),\ i \in \{1, \dots, c\} \quad (7)$$

Для каждого r_i и точки $P_l = R^{i\delta+1}_1 = (P_{l,1} : P_{l,2} : 1)$ выполняется: $r_i(P_{l,1}, P_{l,2}) \ne 0$. Степень каждого r_i равна δ.

b) Пусть теперь $k_1 < c\delta$, причём $k_1 \le \delta$ и $k_1 < c$. Тогда в кольце $\mathbb{F}_q[x_1, x_2]$ рассмотрим следующие многочлены:

$$r_i(x_1, x_2) = (x_1 - R^i_{1,1}),\ i \in \{1, \dots, k_1\}. \quad (8)$$

Для каждого r_i и точки $P_l = R_1^{i+1} = (P_{l,1} : P_{l,2} : 1)$ выполняется $r_i(P_{l,1}, P_{l,2}) \neq 0$. Степень каждого r_i не превышает δ. Рассмотрим множество ненулевых многочленов степени не выше δ, не совпадающих с r_i, $i \in \{1, \dots, k_1\}$. Таких многочленов $q^{\delta+1} - k_1 - 1$ штук. Тогда в качестве r_j, $j \in \{k_1 + 1, \dots, c\}$ возьмём многочлены из этого множества такие, что $r_j(P_{l,1}, P_{l,2}) \neq 0$ для некоторой $P_l = (P_{l,1} : P_{l,2} : 1) \in P$.

c) Пусть теперь $k_1 < c\delta$, причём $k_1 \leq \delta$, но $k_1 \geq c$. Тогда в кольце $\mathbb{F}_q[x_1, x_2]$ можно рассмотреть следующие многочлены:

$$r_i(x_1, x_2) = (x_1 - R_{1,1}^i),\ i \in \{1, \dots, c-1\},\quad r_c(x_1, x_2) = (x_1 - R_{1,1}^c) \dots (x_1 - R_{1,1}^{k_1}). \tag{9}$$

Для каждого такого r_i найдётся точка $P_l = (P_{l,1} : P_{l,2} : 1)$, для которой $r_i(P_{l,1}, P_{l,2}) \neq 0$. Для $i < c$ такой точкой, например, является точка R_1^{i+1}, а для $i = c$ такой точкой является R_1^{c-1}. Так как $k_1 - c + 1 \leq \delta - c + 1 \leq \delta$, то степень каждого r_i не превышает δ.

d) Пусть $k_1 < c\delta$, и $k_1 > \delta$. Тогда в кольце $\mathbb{F}_q[x_1, x_2]$ можно рассмотреть следующие многочлены:

$$r_i = (x_1 - R_{1,1}^{(i-1)\delta+1}) \dots (x_1 - R_{1,1}^{i\delta}),\ i \in \{1, \dots, \lceil \frac{k_1}{\delta} \rceil - 1\},$$

$$r_{\lceil \frac{k_1}{\delta} \rceil} = (x_1 - R_{1,1}^{(\lceil \frac{k_1}{\delta} \rceil - 1)\delta+1}) \dots (x_1 - R_{1,1}^{k_1}). \tag{10}$$

Для каждого такого r_i найдётся точка $P_l = (P_{l1} : P_{l2} : 1)$, такая, что $r_i(P_{l1}, P_{l2}) \neq 0$. Для $i \leq \lceil \frac{k_1}{\delta} \rceil - 1$ такой точкой, например, является точка $R_1^{i\delta+1}$, а для $i = \lceil \frac{k_1}{\delta} \rceil$ такой точкой является $R_1^{(\lceil \frac{k_1}{\delta} \rceil - 1)\delta}$. Так как $k_1 - ((\lceil \frac{k_1}{\delta} \rceil - 1)\delta + 1) + 1 < c\delta - (\lceil \frac{c\delta}{\delta} \rceil - 1)\delta \leq c\delta - (c-1)\delta \leq \delta$, то степень каждого r_i не превышает δ. В качестве r_j, $j \in \{\lceil \frac{k_1}{\delta} \rceil + 1, \dots, c\}$ возьмём произвольные ненулевые многочлены степени не выше δ, не совпадающие с r_i, $i \in \{1, \dots, \lceil \frac{k_1}{\delta} \rceil\}$, такие, что для них существует точка $(P_{l,1} : P_{l,2} : 1) \in P$ такая, что $r_i(P_{l,1}, P_{l,2}) \neq 0$.

Во всех случаях a), b), c), d) степень каждого из многочленов r_i не превышает δ, все многочлены различны и для каждого многочлена r_i найдётся такая точка $P_l = (P_{l,1} : P_{l,2} : 1) \in P$, что $r_i(P_{l,1}, P_{l,2}) \neq 0$.

Рассмотрим проективизацию построенных многочленов $r_i(x_1, x_2)$ и получим однородные многочлены $R_i(X_1, X_2, X_3)$ степени не выше δ. Построим рациональные функции:

$$H_i = \frac{R_i(X_1, X_2, X_3)}{X_3^{\deg(R_i)}}, \tag{11}$$

являющиеся элементами поля $\mathbb{F}_q(\mathcal{X})$. Покажем, что H_i принадлежит пространству Римана-Роха $L(D)$, ассоциированному с дивизором D. Действительно, согласно замечанию 2 из [7], дивизор построенной функции H_i имеет вид:

$$(H_i) = \mathcal{X} \cdot R_i(X_1, X_2, X_3) - \mathcal{X} \cdot X_3^{\deg(R_i)}.$$

В силу замечания к теореме 2.23 из [10]

$$\sum_{M \in \mathcal{X}(F, \mathbb{F}_q)} I(M; \mathcal{X}(F, \mathbb{F}_q); G) \leq \deg(G) \cdot \deg(F),$$

поэтому в силу (2)

$$\mathcal{X} \cdot X_3^{\deg(R_i)} = \textstyle\sum_{M \in \mathcal{X}(F, \mathbb{F}_q)} I(M; \mathcal{X}(F, \mathbb{F}_q); X_3^{\deg(R_i)})M = I(Q; \mathcal{X}(F, \mathbb{F}_q); X_3^{\deg(R_i)})Q$$
$$\leq \deg(X_3^{\deg(R_i)})\deg(F)Q = \deg(R_i)\deg(F)Q.$$

Тогда

$$(H_i) = \mathcal{X} \cdot R_i(X_1, X_2, X_3) - \mathcal{X} \cdot X_3^{\deg(R_i)} \geq \sum_{P_j \in P} I(P_j, X, R_i)P_j - \deg(R_i)\deg(F)Q,$$

$$(H_i) + D \geq \sum_{P_j \in P} I(P_j, \mathcal{X}, R_i)P_j - \deg(R_i)\deg(F)Q + \alpha Q =$$

$$= \sum_{P_j \in P}^{\delta i} I(P_j, \mathcal{X}, \mathcal{P})P_j + (\alpha - \deg(R_i)\deg(F))Q.$$

Так как $\deg(R_i) \leq \delta = \left\lfloor \frac{\alpha}{\deg(F)} \right\rfloor$, то

$$(H_i) + D \geq \sum_{P_j \in P} I(P_j, \mathcal{X}, \mathcal{P})P_j + (\alpha - \left\lfloor \frac{\alpha}{\deg(F)} \right\rfloor \deg(F))Q \geq 0,$$

значит, $H_i \in L(D)$.

III. Построим теперь искомую коалицию $C_0 = \{u_1; \dots; u_c\}$ следующим образом:

$$u_i = Ev_P(H_i) = (H_i(P_1), \dots, H_i(P_n)). \tag{12}$$

Все многочлены r_i различны, поэтому и все R_i, а также H_i тоже различны. Для каждого r_i существует точка $P_l = (P_{l,1} : P_{l,2} : 1) \in P$ такая, что $r_i(P_{l,1}, P_{l,2}) \neq 0$, следовательно, и $H_i(P_{l,1} : P_{l,2} : 1) \neq 0$. Таким образом, в коалиции ровно c различных ненулевых векторов.

IV. Теперь для каждого из рассмотренных на шаге II случаев a)–d) построим искомого потомка ω.

В случае a) коалиция C_0 (см. (12)) в силу (7) и (11) выглядит следующим образом:

$$\begin{cases} u_1 = (0, \dots, 0, H(P_{\delta+1}), \dots, H(P_n)) \\ \dots \\ u_i = (H(P_1), \dots, H(P_{\delta(i-1)}), 0, \dots, 0, H(P_{\delta i+1}), \dots, H(P_n)) \\ \dots \\ u_c = (H(P_1), \dots, H(P_{\delta(c-1)}), 0, \dots, 0, H(P_{\delta c+1}), \dots, H(P_n)) \end{cases},$$

Рассмотрим потомка коалиции C_0:

$$\omega = (0, \dots, 0, \omega_{\delta c+1}, \dots, \omega_n),$$

где для каждого $j \in \{\delta c + 1, \dots, n\}$ значение ω_j задаётся как произвольный элемент из $\{u_{1,j}, \dots, u_{c,j}\}$. Ясно, что $\omega \in \mathrm{desc}(C_0) \setminus C_0$. По построению:

$$|I(\omega, 0)| \geq \delta c = c \left\lfloor \frac{\alpha}{\deg(F)} \right\rfloor.$$

В случае b) коалиция в силу (8) и (11) выглядит следующим образом:

$$\begin{cases} u_1 = (0, \dots, H(P_i), \dots, H(P_n)) \\ \dots \\ u_i = (H(P_1), \dots, H(P_{i-1}), 0, H(P_{i+1}), \dots, H(P_n)) \\ \dots \\ u_{k_1} = (H(P_1), \dots, H(P_{k_1-1}), 0, H(P_{k_1+1}), \dots, H(P_n)) \\ \dots \\ u_j = (H(P_1), \dots, H(P_{j-1}), H(P_j), H(P_{j+1}), \dots, H(P_n)) \\ \dots \\ u_c = (H(P_1), \dots, H(P_{c-1}), H(P_{c+1}), \dots, H(P_n)) \end{cases}$$

Построим потомка ω следующим образом. В качестве ω_i, где $1 \le i \le k_1$, из вектора u_i возьмём ноль, стоящий там на i-ой позиции. Заметим, что для любой позиции j такой, что $j > k_1$, точка P_j лежит в каком-либо классе эквивалентности R^m. Тогда $u_{m,j} = 0$, т.к. по построению значение H_m равно нулю на любой точке из R^m, в том числе на P_j. Значит, для любой такой позиции j мы можем выбрать $\omega_j = u_{m,j} = 0$. Таким образом, комбинированием только первых k_1 векторов мы можем выбрать потомка ω, совпадающего с нулевым вектором. Тогда:

$$|I(\omega, 0)| = n.$$

В случае c) коалиция в силу (9) и (11) выглядит следующим образом:

$$\begin{cases} u_1 = (0, \dots, H(P_i), \dots, H(P_n)) \\ \dots \\ u_i = (H(P_1), \dots, H(P_{i-1}), 0, H(P_{i+1}), \dots, H(P_n)) \\ \dots \\ u_c = (H(P_1), \dots, H(P_{c-1}), 0, \dots, 0, H(P_{k_1}), \dots, H(P_n)) \end{cases}$$

Построим потомка ω. В качестве ω_i, где $1 \le i \le c$, из вектора u_i возьмём ноль, стоящий там на i-ой позиции. Если $c \le i \le k_1$, то в качестве элемента на позиции i возьмём ноль из вектора u_c, также стоящий там на i-ой позиции. Аналогично предыдущему случаю, для любой позиции j такой, что $j > k_1$, точка P_j лежит в одном из классов эквивалентности R^m. Тогда $u_{m,j} = 0$, т.к. значение H_m равно нулю на любой точке из R^m. Значит, для любой такой позиции j мы можем выбрать $\omega_j = u_{m,j} = 0$. Комбинированием всех c векторов мы можем выбрать потомка ω, совпадающего с нулевым вектором:

$$|I(\omega, 0)| = n.$$

В случае d) коалиция в силу (10) и (11) выглядит следующим образом:

$$\begin{cases} u_1 = (0, \dots, 0, H(P_{\delta+1}), \dots, H(P_n)) \\ \dots \\ u_i = (H(P_1), \dots, H(P_{\delta(i-1)}), 0, \dots, 0, H(P_{\delta i+1}), \dots, H(P_n)) \\ \dots \\ u_{\lceil \frac{k_1}{\delta} \rceil} = (H(P_1), \dots, H(P_{(\lceil \frac{k_1}{\delta} \rceil - 1)\delta,1}), 0, \dots, 0, H(P_{k_1}), \dots, H(P_n)) \\ \dots \\ u_c = (H(P_1), \dots, H(P_{c-1}), H(P_{c+1}), \dots, H(P_n)) \end{cases}$$

Построим потомка ω в этом случае. В качестве ω_i, где $1 \le i \le \lceil \frac{k_1}{\delta} \rceil$, из вектора u_i возьмём ноль, стоящий там на i-ой позиции. Если $\lceil \frac{k_1}{\delta} \rceil \le i \le k_1$, то в качестве элемента на позиции i возьмём ноль из вектора $u_{\lceil \frac{k_1}{\delta} \rceil}$, также стоящий там на i-ой позиции. Аналогично предыдущему случаю, для любой позиции j такой, что $j > k_1$, существует номер m такой, что $u_{m,j} = 0$. Значит, для любой такой позиции j мы можем выбрать $\omega_j = u_{m,j} = 0$. Тогда комбинированием первых $\lceil \frac{k_1}{\delta} \rceil$ векторов мы можем выбрать потомка ω, совпадающего с нулевым вектором:

$$|I(\omega, 0)| = n.$$

Итак, во всех вариантах, когда $c\delta < n$, найдётся такой потомок ω коалиции C_0, что $|I(\omega, 0)| \ge c\delta = \min\{c\delta, n\}$.

Таким образом, лемма в случае, когда $c\delta < n$, доказана. Теперь рассмотрим случай, когда $c\delta \geq n$.

Построим коалицию C_0 в этом случае. Пусть $\hat{c} = \lfloor \frac{n}{\delta} \rfloor$, тогда $\hat{c}\delta < n$. Набор многочленов $r_i, i \in \{1, \dots, \hat{c}\}$ и первые $\hat{c}$ элементов коалиции построим так же, как это было описано выше для случая $c\delta < n$ на шагах II и III. Теперь нужно достроить коалицию до необходимой мощности c.

Если на шаге II для $\hat{c}$ реализовались случаи b), c) или d), то, как показано на шаге IV, в качестве потомка построенной коалиции мощности $\hat{c}$ уже может быть выбран нулевой вектор. Поэтому в качестве остальных $c - \hat{c}$ членов коалиции можно взять любые из оставшихся ненулевых кодовых векторов.

Предположим, что на шаге II для $\hat{c}$ реализовался случай a). Если $\hat{c} = \lfloor \frac{n}{\delta} \rfloor = \lceil \frac{n}{\delta} \rceil$, то дополнительных построений проводить не нужно, т.к. в качестве потомка построенной коалиции мощности $\hat{c}$ уже может быть выбран нулевой вектор, и в качестве остальных членов коалиции можно взять любые из оставшихся ненулевых кодовых векторов. Если $\hat{c} = \lfloor \frac{n}{\delta} \rfloor < \lceil \frac{n}{\delta} \rceil$, то построим элемент коалиции с номером $\lceil \frac{n}{\delta} \rceil$ следующим образом. Возьмём проективизацию $R_{\lceil \frac{n}{\delta} \rceil}$ многочлена $r_{\lceil \frac{n}{\delta} \rceil} = (x_1 - P_{(\lceil \frac{n}{\delta} \rceil - 1)\delta + 1,1}) \dots (x_1 - P_{n,1})$ и поделим на X_3^δ, получив рациональную функцию $H_{\lceil \frac{n}{\delta} \rceil}$. Очевидно, что значение $H_{\lceil \frac{n}{\delta} \rceil}$ на точках $P_{(\lceil \frac{n}{\delta} \rceil - 1)\delta + 1}, \dots, P_n$ равно нулю. Аналогично показанному на шаге II в случае $c\delta < n$, проверяется, что $H_{\lceil \frac{n}{\delta} \rceil} \in L(D)$. Тогда можно построить очередной член коалиции $u_{\lceil \frac{n}{\delta} \rceil}$, являющийся образом функции $H_{\lceil \frac{n}{\delta} \rceil}$. По построению на позициях $(\lceil \frac{n}{\delta} \rceil - 1)\delta + 1, \dots, n$ в $u_{\lceil \frac{n}{\delta} \rceil}$ находятся нули. В этом случае оставшиеся $c - \lceil \frac{n}{\delta} \rceil$ членов коалиции выберем как произвольные кодовые ненулевые слова, не совпадающие с построенными ранее членами коалиции. В качестве потомка построенной коалиции может быть выбран нулевой вектор. Действительно, первые $\hat{c}\delta$ позиций могут быть заполнены нулями аналогично случаю, когда $\hat{c} = \lfloor \frac{n}{\delta} \rfloor = \lceil \frac{n}{\delta} \rceil$, а остальные $n - \hat{c}\delta$ позиций можно заполнить нулями, стоящими на соответствующих позициях в векторе $u_{\lceil \frac{n}{\delta} \rceil}$.

Таким образом, построена коалиция $C_0 \in \mathrm{coal}_c(C \setminus \{0\})$. В качестве $\omega \in \mathrm{desc}(C_0) \setminus C_0$ можно выбрать нулевой вектор. Тогда $|I(\omega, 0)| = n \geq n = \min\{c\delta, n\}$.

Итак, лемма доказана и в случае, когда $c\delta \geq n$. □

Доказательство предыдущей леммы довольно громоздко, но содержит описание способа построения по заданной мощности c и кодовому вектору v коалиции C_0 и такого её потомка ω, который совпадает с v не менее, чем в $\min\{c\delta, n\}$ позициях. Этот способ важен при анализе стойкости схем широковещательного шифрования. Проиллюстрируем его на примерах.

Пример 1. *Пусть $\alpha = 7$, $c = 2$. Рассмотрим кривую $\mathcal{X}$ рода $g = 1$, заданную следующим многочленом:*

$$F(X_1, X_2, X_3) = X_2^2 X_3 + X_1 X_2 X_3 + X_2 X_3^2 - X_1^3 - X_3^3$$

над полем $\mathbb{F}_8 = \mathbb{F}_2[\xi]/(\xi^3 + \xi + 1)$. Тогда $\delta = \left\lfloor \frac{\alpha}{\deg(F)} \right\rfloor = \lfloor \frac{7}{3} \rfloor = 2$. Выпишем все точки кривой:

$$Q = (0 : 1 : 0), P_1 = (1 : 0 : 1), P_2 = (\xi : \xi : 1), P_3 = (\xi^2 : \xi^2 : 1),$$

$$P_4 = (\xi^3 : \xi^4 : 1), P_5 = (\xi^4 : \xi^4 : 1), P_6 = (\xi^5 : \xi : 1), P_7 = (\xi^6 : \xi : 1), P_8 = (\xi^4 : 1 : 1),$$

$$P_9 = (\xi^5 : \xi^2 : 1), P_{10} = (\xi^6 : \xi^4 : 1), P_{11} = (\xi^2 : 1 : 1), P_{12} = (\xi^3 : \xi^2 : 1), P_{13} = (\xi : 1 : 1).$$

Рассмотрим АГ-код L-конструкции $C = C(\mathcal{X}, \{P_1, \dots, P_{13}\}, D = \alpha Q)$ и кодовый вектор $v = 0$.

Построим искомые коалицию C_0 этого кода мощности c и потомка ω, используя лемму 3. Классы эквивалентности по первой координате выглядят следующим образом:

$$R^1 = \{P_1\}, R^2 = \{P_2, P_{13}\}, R^3 = \{P_3, P_{11}\}, R^4 = \{P_4, P_{12}\},$$

$$R^5 = \{P_5, P_8\}, R^6 = \{P_6, P_9\}, R^7 = \{P_7, P_{10}\}.$$

Значит, $k_1 = 7 > 1$ и при построении искомой коалиции можно использовать классы R^i. Нумерация точек соответствует наложенному в лемме требованию, что $P_i \in R^i, i \in \{1, \dots, k_1\}$. В нашем случае $c\delta = 2 \cdot 2 < n = 13$ и $c\delta = 2 \cdot 2 \leq k_1 = 7 \leq n = 13$. Такому набору параметров соответствует случай а) на шаге II из леммы 3. Значит, мы можем построить коалицию C_0 и потомка ω такого, что $I(\omega, 0) \geq c\delta = 4$. Многочлены r_i выглядят следующим образом:

$$r_1 = (x - R^1_{1,1})(x - R^2_{1,1}) = (x - P_{1,1})(x - P_{2,1}) = (x - 1)(x - \xi) = x^2 - \xi^3 x + \xi,$$

$$r_2 = (x - R^3_{1,1})(x - R^4_{1,1}) = (x - P_{3,1})(x - P_{4,1}) = (x - \xi^2)(x - \xi^3) = x^2 - \xi^5 x + \xi^5,$$

а R_i выглядят так:

$$R_1 = X_1^2 - \xi^3 X_1 X_3 + \xi X_3^2,$$
$$R_2 = X_1^2 - \xi^5 X_1 X_3 + \xi^5 X_3^2.$$

Тогда H_i выглядят следующим образом:

$$H_1 = \frac{X_1^2 - \xi^3 X_1 X_3 + \xi X_3^2}{X_3^2},\ H_2 = \frac{X_1^2 - \xi^5 X_1 X_3 + \xi^5 X_3^2}{X_3^2}.$$

Из замечания 2 в [7] и теоремы 2.23 в [10] вычисляем:

$$(H_1) = 2P_1 + P_2 + P_{13} - 4Q, (H_2) = P_3 + P_4 + P_{11} + P_{12} - 4Q.$$

Тогда

$$(H_1) + D = (H_1) + 7Q = 2P_1 + P_2 + P_{13} - 4Q + 7Q = 2P_1 + P_2 + P_{13} + 3Q \geq 0,$$

$$(H_2) + D = (H_2) + 7Q = P_3 + P_4 + P_{11} + P_{12} - 4Q + 7Q = P_3 + P_4 + P_{11} + P_{12} + 3Q \geq 0,$$

значит, H_1 и H_2 принадлежат пространству Римана-Роха $L(D)$. Отображение $Ev_P(L(D))$ переведёт H_1 в вектор $(0, 0, H_1(P_3), H_1(P_4), \dots, H_1(P_{13}))$, а H_2 в вектор $(H_2(P_1), H_2(P_2), 0, 0, H_2(P_5), \dots, H_2(P_{13}))$. Коалиция из этих двух векторов гарантированно генерирует потомка ω с $c\delta = 4$ нулями на первых четырёх позициях. Тогда $I(\omega, 0) \geq c\delta = 4$. Искомая коалиция C_0 построена.

Пример 2. *Пусть $\alpha = 5, c = 2$. Рассмотрим кривую $\mathcal{X}$ рода $g = 0$, заданную следующим многочленом:*

$$F(X_1, X_2, X_3) = X_2 - X_3 = 0$$

над полем $\mathbb{F}_8 = \mathbb{F}_2[\xi]/(\xi^3 + \xi + 1)$. Обозначим $\delta = \left\lfloor \frac{\alpha}{\deg(F)} \right\rfloor = \lfloor \frac{5}{1} \rfloor = 5$. Выпишем все точки кривой:

$$Q = (1 : 0 : 0), P_1 = (0 : 1 : 1), P_2 = (1 : 1 : 1), P_3 = (\xi : 1 : 1),$$

$$P_4 = (\xi^2 : 1 : 1), P_5 = (\xi^3 : 1 : 1), P_6 = (\xi^4 : 1 : 1), P_7 = (\xi^5 : 1 : 1), P_8 = (\xi^6 : 1 : 1).$$

Рассмотрим АГ-код L-конструкции $C = C(\mathcal{X}, \{P_1, \dots, P_8\}, D = \alpha Q)$ и кодовый вектор $v = 0$. Отметим, что согласно замечанию 1, этот код является кодом Рида-Соломона.

Построим коалицию C_0 этого кода мощности c, используя алгоритм из леммы 3. Классы эквивалентности по первой координате построим следующим образом: $R^i = \{P_i\}, i = 1, \dots, 8$. Индекс k_1 равен 8. Отметим, что индекс по второй координате равен 1. Легко видеть, что по построению классов необходимая далее перенумерация уже произведена. В нашем случае $c\delta = 2 \cdot 5 = 10 \geq n = 8$. Такому набору параметров соответствует второй случай из леммы 3. В этом случае мы можем построить коалицию C_0 и потомка ω такого, что $I(\omega, 0) = n = 8$. По алгоритму сначала мы должны построить

$\hat{c} = \lceil n/\delta \rceil = 1$ *многочленов по алгоритму из шага II, заменяя* c *на* $\hat{c}$*. В этом случае для* $\hat{c}$ *реализуется случай а) из шага II, когда* $\hat{c}\delta \le k_1 \le n$*. Многочлен* r_1 *выглядит следующим образом:*

$$r_1 = (x - R^1_{1,1})(x - R^2_{1,1})(x - R^3_{1,1})(x - R^4_{1,1})(x - R^5_{1,1}) =$$

$$= (x - P_{1,1})(x - P_{2,1})(x - P_{3,1})(x - P_{4,1})(x - P_{5,1}) =$$

$$= (x - 0)(x - 1)(x - \xi)(x - \xi^2)(x - \xi^3) = x^5 + \xi^2 x^4 + \xi^5 x^3 + \xi^5 x^2 + \xi^6 x,$$

а R_1 *выглядит так:*

$$R_1 = X_1^5 + \xi^2 X_1^4 X_3 + \xi^5 X_1^3 X_3^2 + \xi^5 X_1^2 X_3^3 + \xi^6 X_1 X_3^4.$$

Тогда H_1 *выглядит следующим образом:*

$$H_1 = \frac{X_1^5 + \xi^2 X_1^4 X_3 + \xi^5 X_1^3 X_3^2 + \xi^5 X_1^2 X_3^3 + \xi^6 X_1 X_3^4}{X_3^5}.$$

Из замечания 2 в [7] и теоремы 2.23 в [10] вычисляем:

$$(H_1) = P_1 + P_2 + P_3 + P_4 + P_5 - 5Q.$$

Тогда

$$(H_1) + D = (H_1) + 5Q = P_1 + P_2 + P_3 + P_4 + P_5 - 5Q + 5Q = P_1 + P_2 + P_3 + P_4 + P_5 \ge 0$$

и $H_1 \in L(D)$*. Далее строим* r_2 *по оставшимся* $n - \hat{c} = 3$ *нулям:*

$$r_2 = (x - P_{6,1})(x - P_{7,1})(x - P_{8,1}) = (x - \xi^4)(x - \xi^5)(x - \xi^6) = x^3 + \xi^2 x^2 + x + \xi.$$

Многочлен R_2 *выглядит так:*

$$R_2 = X_1^3 + \xi^2 X_1^2 X_3 + X_1 X_3^2 + \xi X_3^3,$$

а H_2 *выглядит так:*

$$\frac{X_1^3 + \xi^2 X_1^2 X_3 + X_1 X_3^2 + \xi X_3^3}{X_3^3}.$$

Вычислим $(H_2) + D = P_6 + P_7 + P_8 - 3Q + 5Q \ge 0$*, тогда* $H_2 \in L(D)$*. Отображение* $Ev_P(L(D))$ *переведёт* H_1 *в вектор* $(0, 0, 0, 0, 0, H_1(P_6), H_1(P_7), H_1(P_8))$*, а* H_2 *в вектор* $(H_2(P_1), H_2(P_2), H_2(P_3), H_2(P_4), H_2(P_5), 0, 0, 0)$*. Тогда коалиция из этих двух векторов гарантированно генерируют потомка* $\omega = 0$*: возьмём первые пять нулей из первого вектора, а последние три нуля – из второго. Получаем* $I(\omega, 0) \ge c\delta = n = 8$*. Искомая коалиция* C_0 *построена.*

Доказательство теоремы 3.

1. Докажем сначала, что

$$R_{FP}(C) \ge \left\lceil \frac{n}{\alpha} \right\rceil.$$

Для того, чтобы проверить это неравенство, достаточно показать, что если $c < \left\lceil \frac{n}{\alpha} \right\rceil$, то код C обладает c-FP свойством.

Пусть $c < \left\lceil \frac{n}{\alpha} \right\rceil$, тогда $c < \frac{n}{\alpha}$, и $c\alpha < n$. В силу леммы 2 отсюда получаем:

$$\forall v \in C \; \forall C_0 \in \mathrm{coal}_c(C \setminus \{v\}) \; \forall \omega \in \mathrm{desc}(C_0) \setminus C_0 \; : \; |I(\omega, v)| \le c\alpha < n.$$

Значит,

$$\forall v \in C \; \forall C_0 \in \mathrm{coal}_c(C \setminus \{v\}) \; \forall \omega \in \mathrm{desc}(C_0) \setminus C_0 \; : \; v \ne \omega,$$

это и означает, что C является c-FP кодом.

2. Теперь докажем, что если Q – единственная бесконечная точка на кривой $\mathcal{X}$, $|P| > 1$, а $D = \alpha Q$, то

$$R_{FP}(C) \le B_{FP}(C) = \left\lceil \frac{n}{\lfloor \frac{\alpha}{\deg(F)} \rfloor} \right\rceil.$$

Пусть $\hat{c}$ — произвольное целое такое, что $\hat{c} \ge B_{FP}$. Чтобы доказать искомую оценку, достаточно показать, что при числе злоумышленников $\hat{c}$ рассматриваемое FP-свойство не выполнено. В силу (6) из леммы 3:

$$\forall c \in \mathbb{N} \setminus \{1\}\ \forall v \in C\ \exists C_0 \in \mathrm{coal}_c(C \setminus \{v\})\ \exists \omega \in \mathrm{desc}(C_0) \setminus C_0\ :$$

$$|I(\omega, v)| \ge \min\{c \left\lfloor \frac{\alpha}{\deg(F)} \right\rfloor, n\}.$$

По предположению $\hat{c} \ge B_{FP}$, поэтому

$$|I(\omega, v)| \ge \min\{c \left\lfloor \frac{\alpha}{\deg(F)} \right\rfloor, n\} = n.$$

То есть $|I(\omega, v)| = n$, значит, $\omega = v \in \mathrm{desc}(C_0) \setminus C_0$. Это и значит, что FP-свойство не выполнено, следовательно, $R_{FP}(C) \le B_{FP}(C)$.

Теорема 3 доказана.

4. Границы для свойства c-ТА

Сформулируем теорему о границах свойства c-ТА.

Теорема 4. *Пусть $\mathcal{X} = \mathcal{X}(F, \mathbb{F}_q)$ – плоская гладкая проективная кривая. Рассмотрим АГ-код $C = C(\mathcal{X}(F, \mathbb{F}_q), P, D_\alpha)$. Тогда*

$$R_{TA}(C) \ge \lceil \sqrt{n/\alpha} \rceil.$$

Если Q – единственная бесконечная точка на $\mathcal{X}$, $|P| > 1$, $D = \alpha Q$, то:

$$R_{TA}(C) \le B_{TA}(C) = \left\lceil \frac{n + \alpha}{2 \left\lfloor \frac{\alpha}{\deg(F)} \right\rfloor} \right\rceil.$$

Доказательство. Первое утверждение доказано в теореме 1 из [7].

Докажем второе утверждение. Пусть, как и выше в лемме 3, $\delta = \lfloor \frac{\alpha}{\deg(F)} \rfloor$. Для доказательства этого утверждения достаточно показать, что если c – произвольное целое число такое, что

$$c \ge B_{TA}(C) = \left\lceil \frac{n + \alpha}{2\delta} \right\rceil,$$

то C не является c-ТА кодом. Тогда в предположении, что $c \ge B_{TA}(C)$, получаем:

$$c\delta \ge (n + \alpha)/2. \tag{13}$$

Пусть $v \in C$ – произвольное кодовое слово. Согласно определению c-ТА для того, чтобы подтвердить, что это свойство не выполнено, достаточно показать:

$$\exists C_0 \in \mathrm{coal}_c(C)\ \exists \omega \in \mathrm{desc}(C_0)\ \ :\ \forall i \in \{1, \dots, c\}\ |I(\omega, u_i)| \le |I(\omega, v)|.$$

В качестве C_0 и ω рассмотрим построенные в лемме 3 коалицию C_0 и её потомка ω и покажем, что выполняются искомые неравенства. Не нарушая общности предположим, что $k_1 > 1$, и для построения коалиции C_0 использовались классы эквивалентности R^i (см. (4), (5)).

Рассмотрим два случая.

1. Пусть $c\delta \le k_1$. Тогда в силу леммы 3

$$|I(\omega, v)| \ge \min\{c\delta, n\} = c\delta, \tag{14}$$

т.к. $k_1 \le n$. Для произвольного $S \subset \{1, \dots, n\}$ определим $I_S(u, v) = \{i \in S : u_i = v_i\}$. Пусть $A = \{1, \dots, c\delta\}$. Покажем, что

$$\forall i \in \{1, \dots, c\} \; |I_A(\omega, u_i)| \le \alpha. \tag{15}$$

Предположим противное, т.е. найдётся такой номер i_0, что $|I_A(\omega, u_{i_0})| > \alpha$. Тогда существует $r > \alpha$ позиций из A таких, что в каждой такой позиции k выполняется $u_{i_0,k} = \omega_k$. Согласно построению из леммы 3 (см. шаг IV, случай а)), $\omega_j = v_j$ для всех $j \in A$, поэтому $u_{i_0,k} = v_k$. Значит, $|I(v, u_{i_0})| = r > \alpha$. Тогда

$$d(v, u_{i_0}) = n - |I(v, u_{i_0})| < n - \alpha,$$

чего в силу теоремы 1 быть не может, значит, (15) выполнено.

Докажем неравенство

$$|I(\omega, u_i)| \le n - c\delta + \alpha.$$

Ввиду того, что

$$I(\omega, u_i) = I_A(\omega, u_i) \cup I_{\{1,\dots,n\}\setminus A}(\omega, u_i),$$

и неравенства (15) получаем, что

$$|I(\omega, u_i)| = |I_A(\omega, u_i)| + |I_{\{1,\dots,n\}\setminus A}(\omega, u_i)| \le \alpha + n - c\delta. \tag{16}$$

Из (13) вытекает, что

$$n - c\delta + \alpha \le c\delta.$$

Тогда учитывая сначала (16), а потом (14), получим:

$$|I(\omega, u_i)| \le n - c\delta + \alpha \le c\delta \le |I(\omega, v)|.$$

Это означает, что свойство c-TA при данных условиях не выполнено.

2. Пусть $c\delta > k_1$. В случае, когда $k_1 < c\delta < n$, в лемме 3 показано, что $|I(\omega, v)| = n$, т.е. $\omega = v$. Это означает, что C не является c-FP кодом. Аналогично, в случае $c\delta \ge n$ из второго утверждения в теореме 3 вытекает, что код C не является c-FP кодом. Значит, при $c\delta > k_1$ код C не является и c-TA кодом (см. (1)).

Таким образом, показано, что если c – произвольное целое такое, что $c \ge B_{TA}(C)$, то нарушается рассматриваемое TA-свойство. Теорема доказана. □

Если род кривой $\mathcal{X}$ равен нулю, а $\deg(F) = 1$, т.е. код является кодом Рида-Соломона (см. замечание 1), то оценки в теореме превращаются в оценки из [5]:

$$\left\lceil \sqrt{\frac{n}{k-1}} \right\rceil \le R_{TA} \le \left\lfloor \frac{n+k-1}{2(k-1)} \right\rfloor.$$

References

[1] D. R. Stinson and R. Wei, "Combinatorial properties and constructions of traceability schemes and frameproof codes", *SIAM Journal on Discrete Mathematics*, vol. 11, no. 1, pp. 41–53, 1998.

[2] J. N. Staddon, D. R. Stinson, and R. Wei, "Combinatorial properties of frameproof and traceability codes", *Information Theory, IEEE Transactions*, vol. 47, no. 3, pp. 1042–1049, 2001.

[3] A. Silverberg, J. Staddon, and J. Walker, "Applications of list decoding to tracing traitors", *Information Theory, IEEE Transactions*, vol. 49, no. 5, pp. 1312–1318, 2003.

[4] G. A. Kabatyansky, "Traceability codes and their generalizations", *Problems of Information Transmission*, vol. 55, no. 3, pp. 93–105, 2019.

[5] V. M. Deundyak and V. V. Mkrtichyan, "Issledovaniye granits primeneniya skhemy zashchity informatsii, osnovannoy na RS-kodakh", *Diskretn. Anal. Issled. Oper.*, vol. 18, no. 3, pp. 21–38, 2011.

[6] V. M. Deundyak, S. A. Yevpak, and V. V. Mkrtichyan, "Analysis of properties of q-ary Reed–Muller error-correcting codes viewed as codes for copyright protection", *Problems of Information Transmission*, vol. 51, no. 4, pp. 398–408, 2015.

[7] D. V. Zagumennov and V. V. Mkrtichyan, "On application of algebraic geometry codes of L-construction in copy protection", *Prikladnaya Diskretnaya Matematika*, vol. 44, pp. 67–93, 2019.

[8] F. J. MacWilliams and N. J. A. Sloane, *The theory of error-correcting codes*. Elsevier, 1977, vol. 16.

[9] S. A. Evpak and V. V. Mkrtichyan, "Usloviya primeneniya q-ichnyh kodov Rida–Mallera v special'nyh skhemah zashchity informacii ot nesankcionirovannogo dostupa", *Vladikavk. matem. zhurn.*, vol. 16, no. 2, pp. 38–45, 2014.

[10] T. Høholdt, J. H. van Lint, and R. Pellikaan, "Algebraic geometry codes", *Handbook of coding theory*, vol. 1, no. Part 1, pp. 871–961, 1998.

[11] S. G. Vladets, D. Y. Nogin, and M. A. Tsfasman, *Algebrogeometricheskie kody. Osnovnye ponyatiya*. MCCME, 2003.